Strategies to Mitigate Risk in the Current Economic Environment

June 4, 2009

JEFFERSON WELLS
A Manpower Company

Agenda

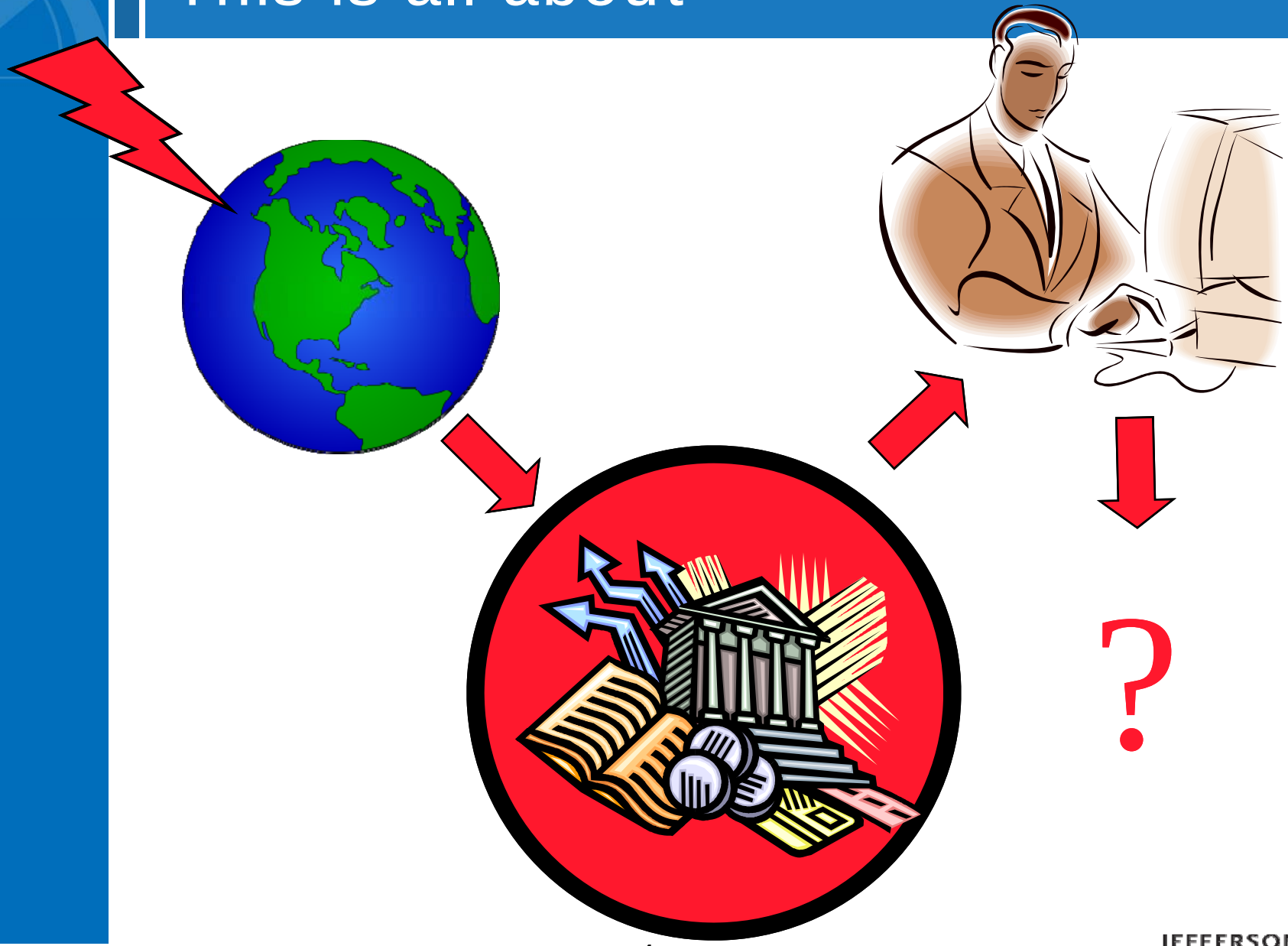
- Introductions
- Rules of the Game
- Overview
- Business
- Technology

Speakers

Randy Watterworth, CPA, CFE, CIA, CISA
Director, Internal Audit and Controls - DFW

Jeffrey Camiel, CISSP, QSA
Director, Technology Risk Management - Texas
20+ years in IT, IT Security and Audit
“Broke it, fixed it, made it better!”

This is all about



This is all about

Predicting

Planning

Protecting

Detecting

When you don't

- 90% of compliance, legal, finance and risk executives surveyed say they expect fraud activity to remain steady or increase in 2009.
- 59% of workers admit that they have downloaded confidential company data for future personal use if they find themselves looking for a new job.
- India leaked credit card #s to BBC News reporters posing as criminals.
- Malware increased by 400% in 2008, a very insidious type of malware that was designed either to steal your data, steal your identity, or steal your money.

And

- 2008 Global Fraud Report -The Economist Intelligence Unit (and Kroll Technology Services)
  - Corporations reported a 22% increase in fraud in 2008 over 2007.
  - Leading causes of the fraud increase:
    - Weakened internal controls
    - High staff turnover
- The San Jose IIA Chapter treasury has suffered an apparent misappropriation of funds.

Reasons for rising threats

- People are concerned about their financial security
- Businesses are failing
- Employees are being told “do more with less”
- Work hours are increasing
- Less room for error as margins narrow
- Increased criminal activity (scams)
- Increased compliance requirements

So what is happening?

- Fraud
- Theft of Intellectual Property
- Loss of Productivity
  - Operations
  - Technology
- Loss of Suppliers
- Loss of Human Capital
- Damage to Brand Name
- Loss of Revenue
- Opportunity Loss
- Physical Harm

So what is happening?

- Employees are packing (theirs and yours)
- Employees are using proprietary information to establish their value to new employers
- Third party services are going out of business
  - See first two
- Criminals are stepping up attack efforts
- Investments are roller coasting

Cost cutting risks

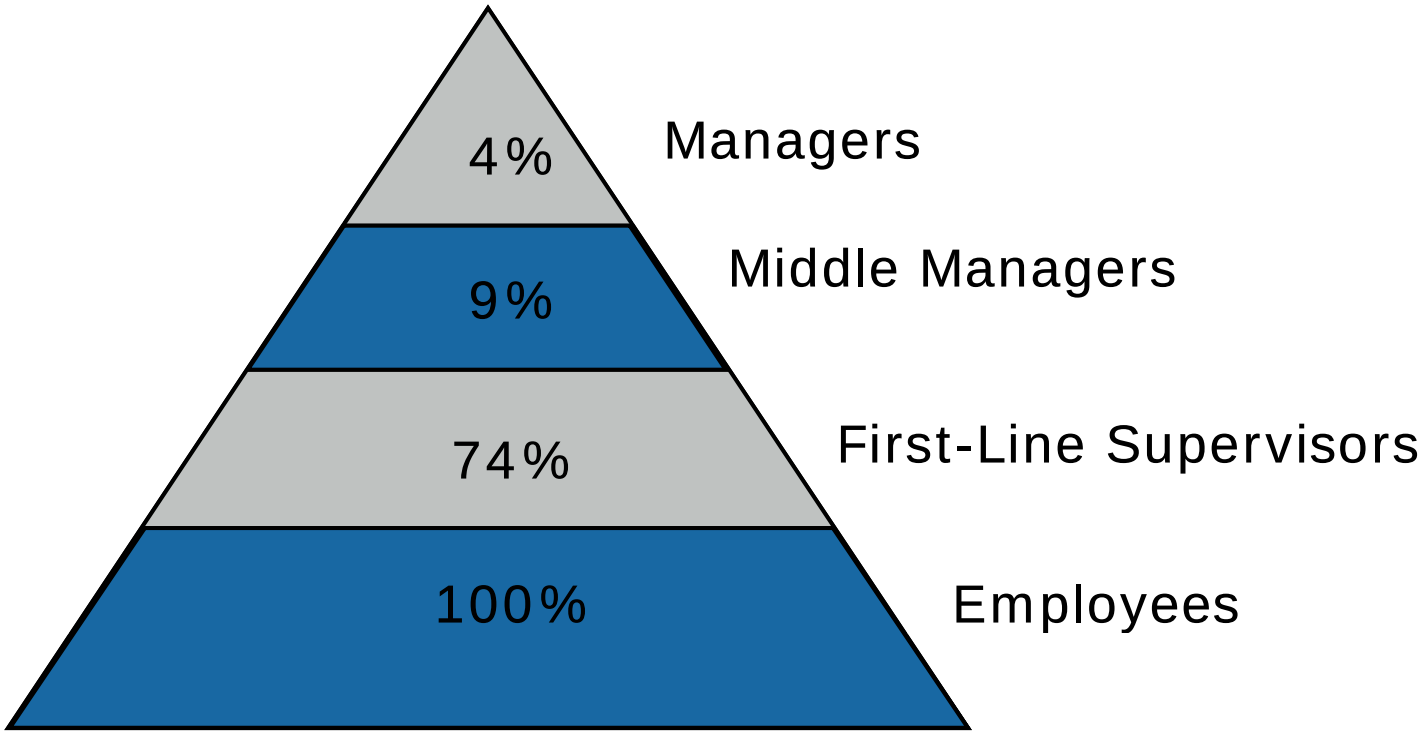
- Poorly managed cost reductions can lead to:
  - Weakened control environment
  - Breakdowns in processes and internal controls (Fraud)
  - Employee morale and retention issues
  - Lost productivity and operational failures
  - Failure to meet business goals
  - Reduction in product and service quality
  - Decrease in competitive position
  - Over-emphasis on cost savings by Internal Audit versus risk based auditing

Risk mitigation – cost cutting

- Cost Cutting Risk Self Assessment
  - Evaluate each cost cutting initiative to ensure:
    - Alignment with overall business strategies
    - Short vs. long term impact
    - Reputational risk
    - Alignment with core principles
    - impact on safety, on related opportunities
    - Stakeholder relationships
    - Skills retention
    - Performance measures
    - Governance systems
    - Control environment

Risk mitigation – cost cutting

- Incent Employees to Provide Cost Reduction Ideas
  - According to a **Bureau of National Affairs Study**, employers that incent companywide cost savings initiatives realized savings of over **$2B!**
  - Why is this important? Pyramid of Ignorance



Risk mitigation – cost cutting

- Benchmark costs with other companies
- Develop a cost "hit list"
- Focus on **REDUCING** Cost of Goods Sold versus G&A
- Identify areas for sustainable cost reductions
  - Consolidate purchases
  - Negotiate lower energy costs, and/or work with suppliers to install energy efficient alternatives
  - Outsource costly, non-core functions to third parties
  - Automate processes to improve productivity and control (T&E reporting)
  - Conduct regular contract compliance, pricing reviews

Risk mitigation – cost cutting

- Limitations of supply-focused cost cutting
  - Unlikely to be rewarded by Wall Street
  - May not be realistic
  - My not be sustainable

- Demand analysis approach to profitable growth
  - Identify products or features that have value to target customers
  - Reduce production costs
  - Improve sales and marketing ROI
  - Volume expansion
  - Increased pricing power

Risk mitigation – cost cutting

- Example: Major food manufacturer increased brand sales from -1% to +15% and returned to profitable growth in one year.
  - Brand costs were reduced by eliminating packaging, supply chain and formulation components not motivating to target consumers.
  - Trade spend was rebalanced to the most profitable, more premium SKUs.

Audit plan additions-cost cutting

- Control deterioration assessments
  - Review controls and process integrity across business units related to cost-cutting measures.
  - Interview line employees - pressures to cut corners to reduce costs.
- Pre-implementation cost-reduction review
  - Examine cost-reduction proposals to ensure they consider:
    - The risk impact to the business beyond cost savings
    - Leave vital company operations untouched

Audit plan additions-cost cutting

- Post-implementation cost-reduction analysis
  - Audit the process by which cost-reduction programs are implemented to ensure adherence to proposed plans and identify new risks as they arise.
- Staff retention audit
  - Review the steps being taken by human resources and middle management to boost retention of high performing staff, such as training and development initiatives and incentive packages.

Human resource risks

- Low engagement of high performers
  - Job satisfaction and employee commitment decrease
  - Career trajectory in jeopardy
- Ineffective retention strategies
  - Compensation-based retention strategies
  - Attrition of high performing employees
- Internal control management deterioration
  - Loss of focus/abandonment of the control environment leaving the company more vulnerable to controllable risks than ever before
- Knowledge management / loss of productivity
  - Poor or non-existent practices used to pass critical process information from a departing employee to a new hire can result in the loss of control and process knowledge
- Fraud and theft

People are Key

A survey by Towers Perrin reveals current widespread anxiety among U.S. employees about job security.

- 45% said they expect their job to change or be eliminated.
- 55% believe their future earnings will plateau or decline.

According to a Forrester Research study on HR Management:

- Labor accounts for 36% of operating costs and 30% of revenues for US companies.
- Employees are the differentiating factor for most firms, and productivity has a great impact on the bottom line.

Risk mitigation–Human Resources

Companies can increase their employee productivity and loyalty by:

- Communicating MORE with employees
- Understanding their workforce attitudes, opinions, motivation and satisfaction
- Helping employees successfully navigate change

Per Dr. Gary Rhoads and Dr. David Whitlark, Allegiance loyalty experts, there are 4 areas that drive employee loyalty:

- being helpful
- feeling confident and improved
- feeling accepted
- feeling respected

Risk mitigation–Human Resources

- Identify critical talent and evaluate turnover risk
- Initiate and hold regular Proactive Discussions on Career Development and retention for critical employees
- Implement Long–term Retention bonuses and/or incentive plans for critical employees
- Offer formal mentoring opportunities with key executives
- Offer job rotations
- Offer opportunities to participate on critical cross functional business strategy, process improvement, system implementation, new business development project teams

Risk mitigation–Human Resources

- Noticing and recognizing the right behaviors is the key to strengthening employee relationships in any economy
- “Recognition is like a small drop of Oil in the machinery of business … it just makes things run a little smoother” Obert C. Tanner, Founder, recognition industry
- Top of all employee’s lists is feeling appreciated
- Simple low cost things you can do:
  - Remember and recognize birthdays
  - Make the most of company’s formal, corporate awards—service, safety and others with a powerful group presentation
  - Find out what inexpensive rewards they value (tickets to a ballgame, a few hours off to spend time with their family)
  - MBWA

Risk mitigation–Human Resources

- Consider evaluating and implementing an HR Management tool or application, which would have the following benefits (Source: Forrester Research):

Process	Strategic benefits	Tactical benefits
Recruiting	▪ Hire better talent ▪ Build a compelling employment brand ▪ Embed Web 2.0 technologies	▪ Reduce cost per hire ▪ Decrease time to hire ▪ Ensure statutory compliance
Learning	▪ Capture and transfer knowledge ▪ Create career plans ▪ Offer varied learning offerings	▪ Manage course curriculum ▪ Management and track course completion ▪ Meet compliance and regulatory requirements
Performance	▪ Create succession plans ▪ Align individual with org. goals ▪ Create consistent competencies ▪ Provide visibility into top performers	▪ Automate the performance review process ▪ Improve performance process compliance and consistency
Compensation	▪ Create a pay-for-performance culture ▪ Ensure pay equity ▪ Forecast future workforce budgets	▪ Price jobs consistent with the market ▪ Prevent overpayments ▪ Manage other incentives ▪ Effectively administer salaries
HRMS	No strategic benefits	▪ Increase efficiencies for highly transactional processes ▪ Manage employee records

Risk mitigation–Human Resources

- Communicate ,Communicate, Communicate

- AND

Communicate some more!

Audit plan additions-Human Resources

- Employee engagement survey
  - Survey employees to assess their understanding of company values and engagement
- High potential talent retention audit
  - Examine HR Department's plans to retain top talent
  - Review the training/development program
  - Evaluate the success in increasing employee engagement and job satisfaction
- Knowledge management audit
  - Evaluate managements' processes to pass critical control and process information from a departing employee to a new hire
- Recruitment strategies review
  - Review recruitment strategies to ensure the company is taking an "activist" approach to acquiring high potential talent
- Succession planning audit
  - Audit succession plan structures at the top levels of the company

A Unique HR opportunity

- There is greater supply of Accounting and Auditing professionals in the job market as compared to prior years.
- Large pool of qualified individuals provides a unique opportunity to supplement or enhance your existing team, providing skill sets that may be missing.
- This is especially critical for Internal Audit, which if a recent E&Y study is correct , may not have all the necessary skill sets required to meet Board of Directors' and management's expectations.

Internal Auditors: Mission Unaccomplished?

- This E&Y research study indicated the following:
  - 57% of companies surveyed said process improvement recommendations were “very important” in meeting management’s expectations for internal audit.
  - Need more focus on strategic and operational risk, don’t just be “compliance police”.
  - Only 17% rated their current team’s skill at enterprise risk assessment as “very competent”.
  - Only 19% said the same for fraud detection, 22% for use of technology and analytics, and 39% for business process improvement.
  - More than a third said it was “very difficult” to recruit people skilled at enterprise risk assessment.
  - A total of 68% said it was very or somewhat difficult to find people knowledgeable about operational auditing or process improvement, compared to 51% for compliance auditing.

Internal Auditors: Mission Unaccomplished?

- E&Y research study (continued):
  - Enterprise risk assessment, fraud detection, use of technology and analytics, and business process improvement should be fundamental and core to any internal auditor.
  - SOX 404 compliance efforts have shifted focus away from these competencies over the past few years; this has created a lack of supply.
  - Attesting on internal controls over financial reporting is management's responsibility, not internal audit.
  - Companies that devote internal audit resources in that direction miss the value traditionally gotten from internal audit, which is alerting you to things that are going wrong, or about to go wrong, or could be improved.

Source: CFO.com, December 4, 2008.

Fraud risks

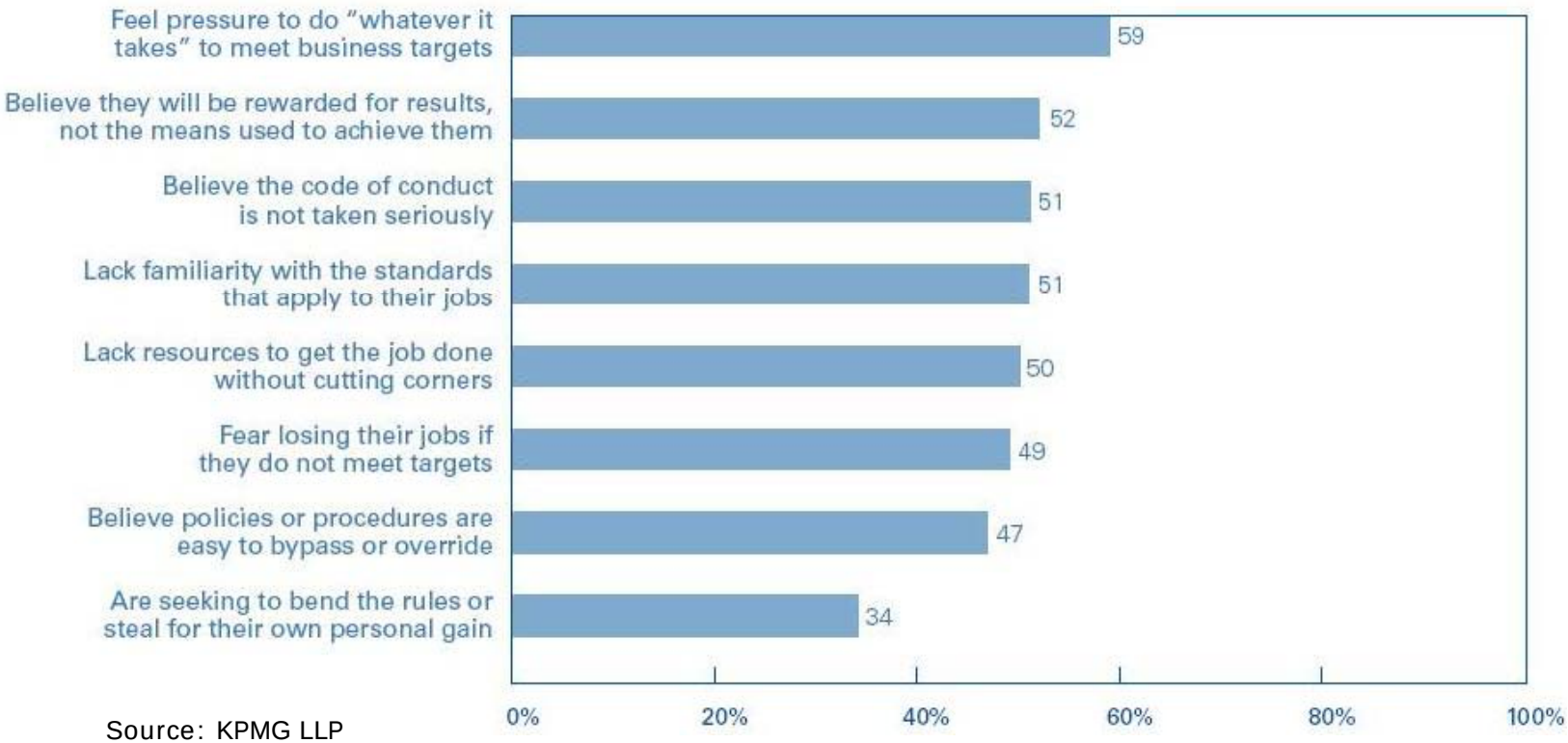
- Tone at the Top
  - Difficult to continue talking about the value of high ethical standards and the importance of individual action when the outlook for the company overall is grim
  - Nervous employees – no trust of the information coming from the top
  - They're willing to do what it takes to protect their jobs
  - Increases the likelihood of fraudulent activity
  - Experts indicate such misconduct can be expected
- Theft - Intellectual Property
  - Market Strategies
  - Contact lists
  - Price Lists
  - R & D
- Financial - Payroll, Inventory, Procurement, Accounts Payable, Financial Reporting
- Reputation - Loss of employee, public, consumer and investor confidence.

Opportunity, pressures, rationalization

- Fraud symptoms include:
  - Missing or altered documents to support transactions
  - Excessive voided documents
  - Transactions without supervisory approval
  - Transactions with inappropriate authorizations
  - Excessive complaints from customers or other employees
  - Unusual billing addresses or arrangements
  - Payments based on photocopied invoices or fabricated invoices
  - Vendor payments sent to an employee's address
- An employee who
  - Is living beyond his or her means
  - Can't manage money
  - Doesn't take a vacation
  - Is dissatisfied with work
  - Is a take-charge person
  - Has expensive habits
  - Has close relationships with customers or vendors

Root Causes of Misconduct

- According to the 2008-2009 KPMG Integrity Survey, major drivers of misconduct include excessive pressures, incentives, uncertainty over the rules, inadequate resources, and job anxiety.



Source: KPMG LLP

Risk mitigation - Fraud

- Fraud Checkup - ACFE
- Letter From CEO
- Antifraud Program
  - Fraud Policy
  - Benchmark Fraud Risk Areas (Annual Surveys, Kroll, ACFE, KPMG)
  - Whistleblower hotline
  - Training
  - Regular Communication
  - Regular targeted audits
- Fraud Risk Assessments
  - At least quarterly
  - Use enabling technology

Elements of an Anti-Fraud Program

- According to the 2008-2009 KPMG Integrity Survey, organizations' antifraud programs included the following specific ethics and compliance program elements:

Source: KPMG LLP

Risk mitigation

- Clear understanding of responsibilities around antifraud programs and controls from the board level down to line employees
- Develop training and communication plans around a Whistleblower program/hotline
- Documented processes for how fraud allegations will be handled at each level
  - Transparent process - Employees must see a process was followed to correct bad behavior, if/when it occurs
  - Enforcement must be swift and sure
  - Ensure that employees see that actions are just as important as words
- Incorporate regular audits of the antifraud program

Audit plan additions – Fraud

- Update fraud risk assessment
  - Target business units that:
    - Face significant job cuts
    - Are financially under-performing
    - Are likely to miss targets/goals in the next 6-12 months
- Physical security/Inventory management audits
  - Areas that pose the greatest risks for employee theft
- Third-party fraud audit
  - Assess ethical behavior of current and potential third-party partners

Typical Fraud Risk Assessment

- "Facilitating a comprehensive fraud and reputation-risk assessment is the single-most important contribution that Internal audit can contribute to an organization's antifraud programs and controls." (PwC, Audit Director Roundtable research)

	Phase	Action Steps	
1	Organize Risk Assessment by Business Cycle	▪ Organize around business process to simplify the assessment	▪ Create a separate cycle for fraud risk assessment
2	Evaluate Fraud Risk Factors	▪ Involve management, Internal Audit, business process owners, IT management and the Audit Committee	▪ Consider past frauds, new frauds, frauds in the industry, weak internal controls, entry in new markets, new products
3	Identify Potential Fraud Schemes and Scenarios	▪ Identify the universe of potential risks ▪ Taylor identified schemes to specific businesses	▪ Consider the risk of overriding controls
4	Assess Likelihood of Fraud and Significance of Risk	▪ Determine if potential fraud risk is remote, more than remote, or probable	▪ Assess the significant of fraud risks that have more than a remote likelihood of occurring and are more than inconsequential
5	Evaluate Whether Mitigating Controls Exist	▪ Determine if controls are in place to sufficiently mitigate identified risks	▪ Map fraud risks to existing internal controls

Audit plan additions – Fraud

- Insider Trading audit
  - Review all major shifts in strategy:
    M&A activity
    Management / leadership changes
- Anti-fraud culture audit
  - Identify areas of weakness
  - Perform surprise audits of the fraud controls in place
- Tone-at-the-top reviews
  - Review messaging and tone from senior management and the board
    - Are they building trust across the organization
    - Are they sending messages that emphasize the values and integrity of the company in managing through difficult times

Tone at the Top

- Evaluate the motivation and opportunity for senior executives to commit financial fraud and the company's overall vulnerability.

Checklist of Fraud Motivation Indicators

	Management Integrity Indicators	Behavior or Characteristic
Subjective Factors	Tone at the top and other inherently subjective management indicators that assess how well management promotes and personally follows an antifraud culture	Executive entertains in a style that could be considered lavish.
		Executive makes extensive use of personal perks (e.g., company aircraft, cars, etc.).
		Executive directs the company's charitable giving to personal pet projects rather than organizations of strategic importance to the company.
		Executive has failed to correct known issues in internal controls.
		Executive fails to effectively communicate and support the company's values or ethics.
		Executive exhibits domineering behavior, especially involving attempts to influence the scope of the auditor's work.
	External Industry / Competitive Indicators	**Behavior or Characteristic**
Objective Factors	External factors that can objectively measure the likelihood or motive for management to commit fraud	The executive's area or the company is subject to new accounting or regulatory requirements that are difficult to interpret and implement.
		The industry is declining and witnessing more business failures.
		Competitors are currently under investigation for questionable business practices.
		The company is experiencing significant margin erosion or a higher degree of competition.

Tone at the Top (continued)

Checklist of Fraud Motivation Indicators (cont.)

Objective Factors

Internal Company Performance Indicators	Behavior or Characteristic
Internal factors that signify a potential operating environment ripe for executive-level fraud	The executive or the company has unusual or highly complex transactions not well understood by Internal Audit.
	The company has an unusual number of legal entities compared to peer organizations.
	A significant portion of management's compensation is dependent on bonuses or other incentives, the value of which is dependent on meeting aggressive earnings targets.
	Executive has not signed the Code of Conduct.
	Individuals directly reporting to the executive have not signed the Code of Conduct.

Source: National Association of Corporate Directors; Audit Director Roundtable research.

Case Study

- Fraud case study in Outsourcing:
  "The Overriding Objective"
  - (if time permits)

Notes

And Now Technology

The Ponemon Institute and Symantec study showed that employees steal the following data:

- 65% E-mail lists
- 45% Included non-financial business information
- 39% Customer contact lists
- 35% Employee records
- 16% Financial information

And

- DAVOS, Switzerland (Reuters) – McAfee Inc. reported businesses risk losing over $1 trillion from loss or theft of data and other cybercrime.
- On December 16, 2008, the “FTC” issued a final consent decree against a mortgage lender, alleging that the lender failed to adequately protect non-public personal financial information provided to a third party.
- Student lender settles FTC charges that it failed to safeguard sensitive consumer information and misrepresented its security practices. As a result of security failures, employees transferred more than 7,000 files with consumer information to third parties without authorization, and one employee sold to the public surplus hard drives that contained, in clear text, information about 34,000 consumers.

Closer to Home

- Ex-Employee Fingered in Company Hack - The FBI is investigating a computer intrusion at a large company that crippled the firm's forecast system costing it over $26,000. The company failed to immediately shut off his VPN access. Someone using the account began logging onto the corporate network, e-mailing out proprietary data to a personal Yahoo account, and modifying and deleting files. The company logs showed that the VPN connection originated at the employees home IP address.

- The FBI is treating the case as a suspected violation of federal computer crime laws, including a rarely-used statute prohibiting breaking into a computer and creating "a threat to public health or safety."

How does that effect me?

- Intellectual property - Why does our competition have our list of client contacts?
- Business continuity - Why did our BCM program fail when the network outage occurred?
- Change management - Why did our financials have errors?
- Support - Why was I not able to reach anyone, when needed help getting remote access?
- Resources - What happened to Bob?
- Resources - What? I have to lay off my best person because they are not on the key project? But they know everything!
- Account management - Why does Bob still have active accounts on critical systems?

So what are you doing?

- Wow look at all that stuff happening!
- Not worried, I'm employed
- Yo, management the sky is falling
- I can't stop authorized people from doing authorized/unauthorized things!

or

- What is changing and where?
- How is the change affecting risk?
- Is risk increasing beyond acceptable limits?
- What proactive actions are we taking to mitigate the risk? Prevent/Detect

The difference between the two:

Out of Control vs. In Control

So where do you start?

- It's a big complicated world!
- Multiple moving parts!
- Interdependencies

QuickTime™ and a
decompressor
are needed to see this picture.

- Leverage, Leverage, Leverage
  - Compliance Documentation
  - Business Continuity Documentation
  - Security Assessments
  - Cost Management Analysis

What should you be doing?

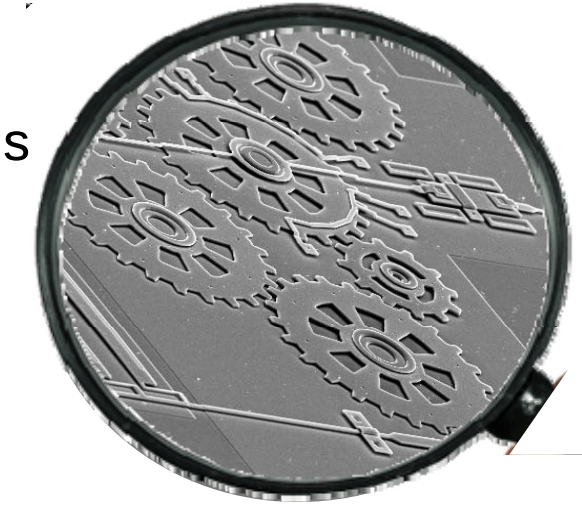
- Protect
  - Service/products delivery
  - Information processes
  - Data integrity and information accuracy
- Prioritize
  - Business processes
  - IT Operations processes
  - Information systems
  - Third-party services
- Identify key knowledge sets
  - Privileged account passwords
  - Key third-party contact information
  - Business continuity procedures
- Monitor
  - Accounts
  - System changes
  - Third-party services

Prioritize

- Business processes
  - Executive/middle management views
  - Compliance requirements
- Applications
  - Business process driven
  - Critical system intersections
- Databases
  - Business process driven
  - Critical information
- Network devices
  - Application architecture driven
- Hardware
- People
  - Supporting prioritized systems
- Third-party services

Analysis

- Critical inventory
  - Key systems
  - Key operations
  - Key third-party services
- Analysis
  - Operations capacity
  - System capacity
  - Key people



- Threat analysis
  - Loss of institutional knowledge
  - Loss of resources - capacity capability
  - Loss of third-party services
  - Loss of intellectual property (proprietary, custodian, third-party hosted)
- Vulnerability analysis
  - “What if analysis” for each item in the inventory?

Common vulnerability strategies

- Communication
- Documentation
- Baselines
- Increased monitoring frequency
- Lowering tolerances
- Forecasting and planning
- Shifting responsibilities

People strategies

- Communication - HR and Information Security
  - Team Meetings
  - E-mail security advisories (positive upbeat)
  - Signage
  - Brown bag lunches
- Message
  - You wouldn't steal a car
  - Theft is theft
  - Reinforcing policies/standards
- Target key people
  - Subject matter experts
  - Administrators
  - Third-party subject matter experts
  - Incentives
- Backup plans
  - Consultants

Knowledge protection strategies

- Industrial knowledge - mainly people based
  - Documentation
  - Cross Training
  - Education
  - System consolidation
  - System standardization
  - ASP models
  - Consultants

Access protection strategies

- Baseline system configurations
- Require higher level of management authority
- Robust termination process
- Restricted account life-spans
- Role/Privilege reviews
- Privileged account password escrows
- Moving to identity management solutions
- Centralized login and failed login monitoring
  - Why is that person logging on in the wee hours of the morning?
- Tying together logical and physical access security monitoring

Data protection strategies

- Baseline permissions
- Application/Database monitoring
  - Who has access?
  - When does that access change?
  - What changes have occurred?
  - Example: Oracle Vault
- Network monitoring
  - Bulk downloads
  - FTP & SFTP transfers
  - Data leakage: Vontu
- Print job monitoring
  - Monitoring capability (application, database, OS, network)
- Host monitoring
  - Is admin access really needed?
  - Example: Tripwire
  - Removable media
- Who monitors? Frequency?

Process protection strategies

- Documentation
- Cross training
- Redundant checks - change management controls, peer as well as management
- Automation
- Consolidation
- ASP/outsource
- Service level agreement reviews
- Business continuity management
  - Planning
  - Documentation
  - Education
  - Testing

Third-party services

- Distance makes the heart have burn
- Periodic financial reviews
- Service level agreements
- SAS 70s II
- Security audits
- Operations audits

This is all about

Predicting

Planning

Protecting

Detecting

The Case

- Company: Smart Stuff Manufacturing Company (SSMC)
- Product: Makers of stuffed animals with embedded artificial intelligence
- Motto: We are always thinking about you!
- Retail: Online, brick and mortar establishments
- Locations
  - Corporate HQ: Cool, California
  - R&D: Palo Alto California
  - Manufacturing and Assembly: Plano, India
  - Retail: Langley, Washington DC, Moscow, London, Hong Kong, New Delhi, Seoul, Kabul, Baghdad
- Data Centers - Dallas, Phoenix
- Employees - 2,500
- Critical Apps - SAP Financial Suite, AIBuild (proprietary), StuffITBuild (proprietary), RetrieveIT

The Case (continued)

- Apps - SAP Financial Suite, Peoplesoft, AIBuildIT (proprietary), StuffITBuild (proprietary), AIProgramIT (proprietary), and RetrieveIT (proprietary)
- 150 servers and virtual instances
  - Retail Locations - 2 servers per, each employee has a laptop
- Virtual workforce enabled
- 2,500 laptops
- Hardline and wireless network infrastructures
- Servers and workstations are all Linux based
- IT employees: 200
- R&D staff: 800
- Sales staff: 300
- Flat network
- LDAP network authentication

The Case (continued)

- You are called in to the CEO's office
- Based on the economy and trending financial trends the CEO informs you that they will be reducing the expense footprint by:
  - Closing retail stores & India manufacturing and assembly plant
  - Consolidating data warehouses
  - Reducing IT by 25%
  - Reducing Sales staff by 50%
  - Reducing India staff by 100%
  - Reducing middle management
- Your new responsibility is to develop a risk prevention plan and present it to the board.
- What do you do?
- What are your risks

This is all about

Predicting

Planning

Protecting

Detecting

Thank You!

Randy Watterworth
Director, Internal Controls
Randy.watterworth@jeffersonwells.com
(office) 214-740-3746
(cell) 254-913-0913

Jeff Camiel
Director, Technology Risk Management
jeffrey.camiel@jeffersonwells.com
(office) 214-740-5515
(cell) 408.310.0549

Notes

Notes